

OECD 消費者政策委員会「オンライン個人情報窃盗に関する報告書」〈抜粋〉

(内閣府仮訳)

2008年1月9日公表

概要

背景

2006年10月の第72回会合にて、消費者政策委員会（CCP）は、のOECD情報・コンピューター・通信政策（ICCP）委員会により実行されたインターネットの未来を形作る幅広い傾向や政策に関する業務を支援するため、オンライン個人情報窃盗の分析を行うことに合意した。この分析は、このような窃盗と闘うためのCCPにおける政策指針に関する2007～2008年の検討をベースとして提示された。これらの原則は2008年6月17～18日に韓国ソウルにてICCPによって開催された閣僚会議で協議される。

分析の構造

分析は5つの章で示されている。

- ・ 第1章の分析は、個人情報窃盗に取り組むためOECD加盟国により採用された異なる法的アプローチと、個人情報窃盗のための個別の刑法罪を作りだすことの影響を調査している。
- ・ 第II章では、個人情報窃盗者たちが被害者の個人情報を得るために使う、社会工学上の技法、悪用のためのソフトウェア（マルウェア）を伴う技術的策略を含む様々な方法について描写する。
- ・ 第III章では、個人情報窃盗者たちが被害者の個人情報を不正使用する様々なやり方について描写する。
- ・ 第IV章は、個人情報窃盗被害者のプロフィールを提供する。これは、被害者の苦情と損失の傾向を反映した統計データを得られるようにするためである。また、個人情報窃盗がオンラインよりもオフラインで蔓延しているかどうかを問うものである。
- ・ 第V章は、個人情報窃盗を抑止するための、加盟国と国際的な執行の成果を示している。

識別情報窃盗の定義

識別情報窃盗の定義は加盟国によって違う。別個の犯罪という見方もあれば、他の犯罪や不正行為を犯す予備段階とみなす国もある。この報告書では、以下の定義が使われている。

識別情報窃盗は、当事者が、未許可の方法により、詐欺や他の犯罪を犯す目的で、または詐欺や他の犯罪に関連して、自然人あるいは法人の個人情報を得る、移す、所有する、また使用する場合に発生する。

この定義は、識別情報窃盗に用いられた媒体に関係なく適用する。この定義は個人と法人両方を含むが、この報告書では消費者に影響する識別情報窃盗（個人情報窃盗）に限り焦点を当てる。

個人情報窃盗のオンラインツールキット

通常、個人情報窃盗者たちは、被害者の個人情報を得るため様々な異なる方法を使う。いくつかのオンラインツールは、自分や他者のシステムに被害を招く目的でインストールされたプログラムである、悪用ソフト（マルウェア）の作動を含む。「フィッシング」は、偽物のメールを送ることでインターネットユーザーを釣り上げ、偽のウェブサイトを使いユーザーが個人情報を開示するよう罠にかけることである。またフィッシングに使用するメールは迷惑メールとして広く配信され、しばしば受信者のコンピューターに悪用ソフトをインストールする。

フィッシング技法はより巧妙となり、見つけることが困難となっている。主な形は以下の通りである。

- ・ 「ファームिंग (pharming)」タイプのメッセージは、通常のフィッシング攻撃と同じ種類の偽IDを使い、同時に、ユーザーを本物のウェブサイトから外見を複製した詐欺のサイトへ誘導する。
- ・ 「スミッシング (SMiShing)」は携帯電話のユーザーがテキストメッセージ (SMS) を受け取り、会社がそのサービスの一つにユーザーが同意したことを確認すると、ユーザーが会社のウェブサイトでキャンセルしない限り、1日あたり一定の料金が課されるというものである。
- ・ 「スピアフィッシング (Spear-phishing)」は、同僚のパスワードやユーザー名を盗むためにある企業の従業員または雇用者に扮し、最終的に企業のコンピューターシステムにアクセスするというものである。

個人情報窃盗の異なる形

個人情報窃盗者は増長した多様で異なる不法なスキームで、被害者の個人情報を不正使用する。通常はこれらのスキームには既存の口座を不正使用すること、不正に新しい口座を開設すること、政府による手当、サービスや政府文書を不正に得ること、健康保険詐欺、個人データの許可なしでの仲介を含む。

オンライン個人情報窃盗の規模を測ることの困難さ

統計は国によって様々に集められているが、国境を越えた比較は複雑である。さらに、公的機関と民間企業によって集められた統計は大きく異なる。ある情報では個人情報窃盗は近年減少しつつあると結論付けて、消費者の信頼が増しているという結果であるが、反対

に、別の情報では個人情報窃盗の増加を反映した数字を提出している。

国内執行戦略

多くのOECD加盟国は公的機関、民間部門で、個人情報窃盗抑止のための消費者とユーザーの教材を策定している。いくつかの国では、個人情報窃盗の捜査を進めるため、様々な公的、民間の団体と情報を共有している。しかしながら、警察機関への情報は、多くの国で限られている。

いくつかの国の企業は、データ漏洩を防ぐための安全保障戦略と人的資源の配置が必要であると理解している。しかしながら、もっと十分にこれらのデータ漏洩を防ぐ企業の努力がなされる必要があるという認識もある。数カ国では、企業やインターネットサービスプロバイダー（ISP）のようなデータ収集者に、公共や関係する顧客に影響を及ぼす漏洩を開示する義務を課す方向で検討段階に踏み出している。大多数の国ははまだ、このような情報開示は法を通してだけ取り入れるべきかどうかを考慮している。欧州連合の加盟国のいくつかでは、ISPはもし顧客の個人情報が悪用され、直接あるいは間接的に損害をこうむる結果になる場合、顧客に代わって行動する権利を要求している。

国際的な執行

政府間のイニシアティブ

様々な国際機関と団体がサイバー詐欺との闘いに取り組んでいる。例えばOECDでは、個人情報、安全性、迷惑メール、消費者に対する詐欺の分野に対応する政策を策定している。その文書は1999年の電子商取引ガイドライン、2003年の越境詐欺ガイドライン、2002年の情報システムとネットワークの安全性ガイドライン、1980年の個人情報保護ガイドライン、2006年の迷惑メールに対するツールキットを含んでいる。

国際通信連合とアジア・ヨーロッパ会議（ASEM）はオンライン上の脅威に対する闘いに関連したもう一つの間である。インターポール（国際犯罪を抑止するための警察組織）は、オンライン犯罪の多国間捜査を実行する上で、各国警察間の協力の基盤としての役目を果たしている。

加えて、オンライン個人情報窃盗を防ぎ、これに訴追するために政府、警察、法執行の力を合わせた、多数の二国間、多国間、地域のスキームがあります。

公-民による国際執行イニシアティブ

民間企業は様々なイニシアティブの下、サイバー攻撃に取り組むため、公的機関の試みに協力しています。いくつかの企業は悪用ソフト、フィッシング、その他のオンライン上の

脅威についての統計をまとめたデータを公的機関と共有する場を持っている。実行に協力している企業もある。政府の捜査を助け、適合的な技術手段を実行し、オーダーメイドの立法の発展と、オンライン環境における個人情報窃盗抑止を目的としたベストプラクティスを推奨することを提案している。

課題

この分析では利害関係者がオンライン個人情報窃盗と闘うための能力を向上させる多くの課題と取り組むことを考えるべきであると提案している。

- ・ **定義** 共通の定義の欠如が、包括的な体系で国境を越えてオンライン窃盗を抑止することの取り組みを複雑にするかもしれない。
- ・ **法的地位** 個人情報窃盗/詐欺は多くのOECD加盟国でそれ自体法的な罪にならない。少数の国では犯罪とみなされる。個人情報窃盗が独立した罪として扱われるかどうか、犯罪とみなすかどうか、検討される必要がある。
- ・ **民間との協力** 民間機関は闘いに活発に参加するべきである。加盟国は個人情報窃盗者に課される罰が増えるように、より限定された法律の制定を考慮することができる。民間部門の支援に従事し、団体を奨励するために、①意識改革キャンペーン、②産業のベストプラクティスを発展させる、③個人情報窃盗の発生率を減らすための技術的解決法を実行し開発する、などである。
- ・ **標準** 加盟国は、民間部門に対するデータ保護義務と、顧客データを持っている企業と他の機関に対しデータ漏洩を開示する義務を課すための、国家基準の確立を試行するべきである。
- ・ **統計** 個人情報窃盗は（オンラインでもオフラインでも）統計学者の興味を惹くことに失敗した。ほとんどのデータはアメリカからなので、欧州の統計データはイギリスを除いて存在しない。データが利用できても個人情報窃盗を独立した犯罪としてカバーしておらず、米国はとりわけ個人情報窃盗を個別の罪として分析したデータの見られる数少ない国である。OECD加盟国全体をカバーしたもっと詳細な、正確な統計データを提示することは、デジタル市場の個人情報窃盗の影響を決定する上で助けになるであろう。
- ・ **被害者支援** 加盟国は被害者を助け、個人情報窃盗の被害から回復させ、被害を最小限にするための被害者支援プログラムの開発を考慮できる。
- ・ **救済案** 加盟国は個人情報窃盗被害者により効果的な法的救済を提供する法律を制定するかどうか考慮できる。
- ・ **抑止と法執行** 個人情報窃盗を禁止する刑法の不足と限られた法執行機関の人的資源は抑止力の不十分さを意味する。加盟国は法執行、個人情報窃盗の捜査と訓練のための資源を増やすことの価値を検討することができる。個人情報窃盗技術と手段の急速な進歩が一般的になるにつれて、この闘いに関与する全てのOECD諸国の機関に、より一層の人的資源と訓練が与えられうるだろう。

- **教育** 消費者、ユーザー、政府、企業、経営者を含む全ての利害関係者をカバーするために個人情報窃盗についての幅広い教育が与えられることを検討しうる。
- **調整と協力** 個人情報窃盗に対する規則及び慣行に関する執行に係る機関は国内外レベルで多数ある。協力への各自の役割と枠組みは彼らの実効性の強化を助けることがはっきりしている。個人情報窃盗の犯罪捜査に専念する国家センターを設置することで国内での法執行の調整を改善するという考えもあるであろう。海外の法機関との調整と協力に関しては、加盟国は、①抑止の強化、②主要な国際機関（サイバー犯罪欧州会議委員会）の参加拡大、③捜査協力要請への対応の改善、④国外パートナーとの協力強化（法執行訓練の場においてなど）、のような相互の関心領域を探求できうる。